Examen de evidencia en Pericias Informáticas Judiciales

Juan Manuel Luzuriaga, jluzuria@jusneuquen.gov.ar

Perito Informático Oficial - Poder Judicial de Neuquén – Gabinete Técnico Contable
Santiago del Estero 64 - Neuquén Capital (8300) - ✍ 4482236

Abstract

*El campo de las pericias informáticas es tan vasto que abarca desde el análisis de contratos de tecnología informática hasta el análisis de equipamiento utilizado para cometer delitos o víctima de ataques a su integridad. Desde el punto de vista práctico, la mayor cantidad de pericias informáticas en causas judiciales se concentran en detectar pruebas de delitos, en donde se hayan utilizado herramientas informáticas para generar documentación. La tarea del perito no debe ser solo proveerle al juez esta información, sino también la garantía de que el proceso realizado para la recolección de la misma no invalida la prueba y es claramente trazable y reproducible. Aquí se propone un modelo de procedimiento para examinar medios de almacenamiento, basado en el procedimiento definido por el IACIS [1] (*International Association of Computer Investigative Specialist *) el cual fue extendido para incrementar la propiedad de trazabilidad***.**

Palabras Clave: Informática Forense – Pericias Informáticas – Trazabilidad - Procedimiento

1 Introducción

Es un hecho que durante la última década las intrusiones e incidentes de seguridad han crecido de manera exponencial estableciendo un escenario oscuro sobre la seguridad de las infraestructuras de computación en el mundo[2]. En este sentido, las organizaciones han adelantado análisis de sus seguridad, instalado múltiples mecanismos de protección y efectuado múltiples pruebas con el fin de mejorar las condiciones de seguridad existentes en cada uno de sus entornos de negocio. Sin embargo, dado que la seguridad completa no existe, siempre esta la probabilidad cierta para un nuevo incidente de seguridad, por lo tanto, cuando éste se presenta, se verifica en un alto porcentaje que las organizaciones no se encuentran preparadas para enfrentar la realidad de una intrusión o incidente.

Por un lado, un incidente representa un reto de la gerencia corporativa para demostrar la diligencia de su organización para enfrentar el hecho, tomar el control, recoger y analizar la evidencia, y finalmente generar el reporte sobre lo ocurrido, que incluye las recomendaciones de seguridad y concepto sobre los hechos del incidente. Por otro, es un compromiso de las instancias técnicas por estar preparadas para actuar y regular el efecto que dicho incidente puede ocasionar a la corporación.

Estas dos visiones, nos ofrecen un marco de reflexión alrededor de la seguridad y la preparación requerida por los profesionales que se encuentran a cargo de las funciones de seguridad informática en las organizaciones. En este sentido, administrar un incidente de seguridad requiere experiencia y habilidades técnicas para controlar las acciones del atacante, pero al mismo tiempo **habilidad y pericia**

para establecer los rastros y registros de dichas acciones con las cuales relacionar las acciones y efectos ocasionados por el intruso dentro del sistema.

Si bien, la seguridad es el principal motivador de las investigaciones en el ámbito de la informática forense, existe otro punto de motivación no menos importante, y estos son los delitos penales que se cometen con la ayuda de herramientas informáticas, en donde la informática "registra" pruebas del proceso delictivo, aquí podemos encontrarnos por ejemplo con el examen de medios de almacenamiento de una computadora personal, en búsqueda de comprobantes de pago fraguados, o de una contabilidad "paralela". Obviamente en estos ejemplos, la seguridad de éstos equipos no se ve comprometida, dado que los propietarios de los equipos informáticos, saben que esta ocurriendo en sus computadoras, las cuales están siendo utilizando adrede para cometer ilícitos.

Considerando que la Informática o Computación forense es la ciencia de adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y guardados en un medio computacional [3], en éste documento nos concentraremos en la obtención buscando darle el atributo de trazabilidad a este proceso

2 Registros informáticos

Al igual que los registros en papel, los registros informáticos no son monolíticos, dado que las cuestiones de evidencia limitarán los tipos de registros informáticos que serán admitidos en el ámbito judicial. Por ejemplo, un registro informático que contenga texto puede ser dividido en 2 categorías: Registro generado por computadora y registro almacenado en una computadora [6], la diferencia radica en quien **generó el contenido del registro,** si una computadora o una persona. Los registros almacenados en una computadora refieren a documentos que contienen los escritos de alguna persona o personas y que ocurrieron de una forma electrónica como por ejemplo mensajes de E-mail, archivos de procesadores de texto o mensajes de chat en Internet. Al igual que otros testimonios o evidencia documental que contienen actos realizados por personas, estos registros almacenados en computadora son generalmente el tipo de registro candidato a ser admitidos para probar la verdad de el hecho investigado, y cuando ocurre esta admisión por parte de la justicia, quien ofrece éstos registros debe mostrar las circunstancias que indican su veracidad y autenticidad.

Sin embargo los registros generados por la computadora contienen la salida de programas, no alterada por la mano humana. Los registros de "log-in" de los ISP (Proveedor de Servicio de Internet), registros telefónicos, y los de ATM (cajeros automáticos de banco) serían los ejemplos mas comunes de este tipo de registros. A diferencia de los registros almacenados en computadora, los que son generados por ésta no contienen actos directos realizados por personas. Si bien un programa de computadora puede crear registros a partir de eventos o estímulos generados por las personas, como puede ser el registro de un ATM respecto de un depósito de $2000 a las 03:00 AM, en éste caso los programas funcionan por sí solos, lo cual pone un interrogante en la autenticidad, el cual debe dilucidarse.

Finalmente existe una tercera categoría de registros informáticos[6]: muchos registros son combinación de los generados y los almacenados en computadora. Por ejemplo un sospechoso en un caso de fraude pude utilizar un programa de planilla de cálculo para procesar figuras financieras relacionadas con un esquema fraudulento. Un registro informático que contenga la salida del programa derivaría de los

actos de la persona sospechosa de realizar las entradas en el programa y el procesamiento de la computadora (las operaciones matemáticas del programa de planilla de cálculo). Debe notarse que en esta categoría existe una transformación de la información ingresada por la persona, la cual es realizada por un programa, cosa que no ocurre con un procesador de texto o un mensaje de E-mail. Entonces en este tipo de registros debe tratarse especialmente la cuestión de autenticidad de dicha transformación, ya que ésta autenticidad dependerá de la correctitud del programa utilizado, considere que un programa que contiene errores condicionará la autenticidad del registro generado.

3 Trazabilidad

La trazabilidad es la propiedad de dejar rastros del proceso que se va realizando, de manera tal que dicho proceso pueda ser reproducido lo mas parecido posible a la primera ejecución. Lo que se busca es que ante la necesidad de una reproducción de dicho proceso, las cosas no sucedan por coincidencias o deducciones sino porque se sabe claramente que paso dar y cómo darlo.

Este concepto implica que debemos poner especial cuidado en la documentación que se debería generar durante la investigación forense, definiendo qué documentar, cómo documentarlo y en que momento hacerlo, ya que ésta debe servir como fuente suficiente de conocimiento para reproducir los pasos de la investigación que produjeron una prueba válida del delito en cuestión. En tal sentido, existen momentos claves de la investigación en los cuales debe registrarse determinada información inherente al proceso que se esta realizando, como se podrá apreciar en el procedimiento propuesto mas adelante.

En el marco de un proceso judicial, este atributo debiera considerarse condición necesaria en las pericias informáticas, dado que generalmente a la "parte" que no le beneficie el dictamen pericial, buscará rebatir los argumentos que dieran lugar a las conclusiones periciales. Por lo tanto el perito debe ser capaz de reproducir fidedignamente todos los pasos que lo llevaron a obtener el dictamen pericial. Es por esto que una pericia trazable contribuye a su solidez procesal.

4 Recolección y preservación de la evidencia

El procedimiento para la recolección de evidencia varía según el país, sin embargo existen una guía básica común para asistir al investigador forense, en donde el hardware es uno de los elementos que se deben tener en cuenta a la hora de la recolección de evidencia, debido a que puede ser utilizado como instrumento (ej. Adulteración de comprobantes de pago), como objetivo del crimen (Ej. Robo de información confidencial), o como producto del crimen (Ej: contrabando), en tal sentido deben hacerse las consideraciones del caso, preguntándose qué partes se deben buscar o investigar.

La recolección de evidencia informática es un aspecto frágil de la computación forense, especialmente porque requiere prácticas y cuidados adicionales que no se tienen en la recolección de evidencia convencional, como bien expone Gomez [4]:" en la mayoría de los casos, los allanamientos son realizados por personal policial que no cuenta con los conocimientos necesarios para la identificación de potencial evidencia digital. Actualmente existen guías de procedimiento que intentan cubrir los

puntos más relevantes, como la Guía del United States Secret Service, o la del Australasian Centre for Policing Research entre otras "
No obstante como mínimo deberían considerarse los siguientes aspectos:

- Tener la precaución de recolectar **todas** las piezas necesarias para la investigación
- Proteger el equipamiento recolectado del daño físico (Ej: Adecuado embalaje para el transporte)
- Proteger la información contenida dentro de los medios de almacenamientos, de causas ambientales (ej. Calor, humedad, campos magnéticos, etc)

5 Procedimiento de examen Forense

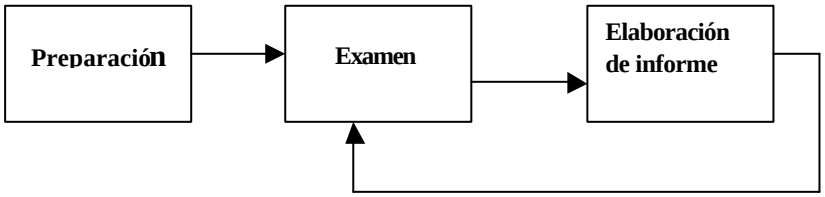
Como postula el IACIS [1], los exámenes forenses de medios de almacenamiento que se practican a cada computadora son diferentes y no deben ser conducidas de la misma manera por numerosas razones., en tal sentido las estrategias de búsqueda dependen del rol que ocupe el hardware investigado: si éste es la evidencia, o fue utilizado como instrumento, o contrabando, o producto del crimen. [5] Generalmente, cuando es posible, el investigador forense debiera planificar conjuntamente con el Juez el secuestro del hardware y analizar su contenido en el laboratorio.

Sin embargo hay 3 requerimientos esenciales para un examen forense:

1. Utilizar medios de examen que posean la propiedad de esterilidad forense (no contaminados)
2. El examen debe mantener la integridad del medio original
3. Deben marcarse , controlarse y transmitirse apropiadamente las Impresiones, copias de datos y pruebas que sean producto del examen

Veamos entonces como deben conducirse estos exámenes para cumplir paso a paso con estos 3 requerimientos, y además incrementar la propiedad de trazabilidad expuesta anteriormente

El procedimiento que se propone, cuenta con un ciclo de vida de 3 etapas, como se ilustra en la siguiente figura



5.1 Examen de medios de almacenamiento

I Preparación

1. El examen de medios se debe realizar en un ambiente Forense sano. Un ambiente Forense sano es aquel que esta completamente bajo el control del examinador,: ninguna acción se toma sin que el examinador permita que ella suceda; y cuando ésta sucede el examinador tiene que poder predecir con certeza razonable cual será el resultado.
2. Establecer condiciones de esterilidad forense. Es decir que todos los medios a utilizar durante el examen deben inicializarse, limpios de información no esencial para la investigación, escanéo de virus y verificados antes del uso. Confeccionar un "check-list" con los puntos necesarios que lleven al investigador a cumplir con estas condiciones.
3. El software a utilizar debe estar correctamente licenciado o autorizado para quien lo utilice, ya sea el examinador o la organización.
4. La computadora objeto de la investigación debe examinarse físicamente, documentando los componentes de hardware, destacando cualquier anomalía o situación inusual hallada durante el examen físico. A tal efecto el investigador deberá documentar un inventario que refleje el examen realizado
5. Tomar las precauciones que se consideren necesarias durante la copia o acceso a los medios originales, a fin de prevenir transferencia de virus que pudiera tener el medio examinado, programas destructivos, u otras escrituras que pueden ser inadvertidas desde o hacia el medio examinado. Documentar versión de todo el software (antivirus, herramientas forenses, etc.) utilizado así como las funciones, configuraciones y parámetros utilizados en cada uno de ellos

II Examen

6. Chequear el contenido de la CMOS, así como el reloj interno verificando la correctitud de fecha y hora. Este último punto suele ser muy importante al momento de establecer la fecha y hora de creación y/o modificación de archivos. Documentar, fecha, hora, dispositivos definidos y otra información que se considere relevante para la investigación. Comparar con el documento obtenido en el punto 4
7. No utilizar normalmente el medio original para el examen . En tal sentido realizar una copia binaria o imagen del medio a analizar, para luego examinar sobre dicha imagen, si el dispositivo cuenta con protección para escritura, esta debe ser activada (ej floppy disk, zip disk, etc). Debe documentarse detalladamente el proceso utilizado para obtener la copia binaria o imagen, incluyendo software detallando la versión, configuración y funcionalidad utilizadas. Así como la descripción del medio original en cuanto a particiones si es HD (Hard Disk), sesiones de escritura si es CDRom.

8. Certificar la copia realizada mediante una "Función Resumen" del tipo de las utilizadas para firma digital como por ejemplo MD5

9. Examinar la copia del medio original, y documentar los puntos encontrados que se consideren de relevancia para la documentación, así como c/u de los pasos utilizados para obtener esta documentación relevante. Aquí es donde la trazabilidad debe ser rigurosa .

10. Examinar el área de boot, la configuración del sistema realizada por el usuario (Ej Windows: Config.sys, autoexec.bat, Ej Unix: /etc/rcd)

11. Recuperar todos los archivos borrados posibles.

12. Listar todos los archivos contenidos en el medio examinado, contengan o no evidencia potencial.

13. Examinar el espacio no utilizado (unallocated space) así como el area "slack" (porción del cluster no utilizada por el archivo) de cada archivo, en busca de datos perdidos u ocultos. Documentar el proceso utilizado para examinar y la información recuperada que se considere de interés para la investigación

14. Examinar especialmente el contenido de los archivos de datos de usuario que puedan ser "vistos" sin el aplicativo que los generó, el directorio raíz y cada subdirectorio. Documentar el proceso utilizado para examinar y la información recuperada que se considere de interés para la investigación

15. Desbloquear y examinar los archivos protegidos con Password . Documentar el proceso utilizado para desbloquear y examinar, así como la información recuperada que se considere de interés para la investigación

16. Examinar los programas ejecutables y los archivos de datos de usuario que solo se acceden con dichos programas. Documentar el proceso utilizado para examinar y la información recuperada que se considere de interés para la investigación

III Elaboración del Informe

16 Imprimir una copia de todo lo que resulte como aparente evidencia, así como su ubicación. Clasificar, identificar, asegurar y transmitir todas las pruebas.

17 Analizar la Información recuperada considerada de interés para la investigación y documentar apropiadamente los comentarios, búsquedas y conclusiones .

18 Si surgen dudas o falta de elementos al momento de elaborar las conclusiones, es recomendable volver a la etapa de examen, para profundizar o complementar la investigación

5.2 Exámenes limitados

Existen instancias en que todos los datos o medios pueden no estar autorizados, no disponibles, no ser conducentes, no ser necesarios, etc. En estos casos el examinador debe documentar en su informe pericial las razones por las cuales no realizó un examen completo. Algunos ejemplos de éstos casos son:

El alcance del examen esta limitado por la solicitud judicial.

El equipamiento debe examinarse in-situ . (Puede requerir que el examen se realice sobre el medio original. Extremar las precauciones en este tipo de examen)

El tamaño del medio es tan grande que un examen completo no es posible.

El peso de la evidencia ya encontrada es tan grande que una búsqueda adicional no es necesaria..

No es posible conducir un examen completo debido a que el hardware, sistema operativo u otras condiciones, sobrepasan los límites del examinador

6 Conclusiones

Si bien existen diversas formas de conducir una investigación forense, en las distintas guías que pueden encontrarse no siempre se contempla en éstas mantener la validez de la prueba para un proceso judicial, puede darse el caso en que la prueba sea contundente, pero si quien la halló no puede repetir sólidamente el proceso mediante el cual fue encontrada (trazabilidad), y demostrar mediante el proceso utilizado que dicha prueba no sufrió alteración alguna, probablemente no sea valorada por el juez al momento de dictar sentencia. Aquí se ha expuesto un procedimiento a seguir para conducir la investigación forense de una manera aceptable para el proceso judicial, de modo que el trabajo pericial informático no sea rechazado por cuestiones de forma.

A futuro, continuando con ésta línea de investigación, se trabajará en la definición de un método integral. para realizar pericias informáticas, que abarque las 4 etapas de la computación forense: adquirir, preservar, obtener y presentar[3]

Referencias

[1] International Association of Computer Investigative Specialist, Disponible en http://www.cops.org/forensic_examination_procedures.htm

[2] Cano Jeimy J.,"Credenciales para investigadores forenses en informática Certificaciones y entrenamiento" Disponible en http://www.acis.org.co/Paginas/publicaciones/jeimy/art-certFore.html

[3] McKemmish, R., "What is Forensic Computing". Trends and Issues in Crime and Criminal Justice(118), ISBN 0 642 24102 3 ; ISSN 0817- 8542, 1997. Disponible en: http://www.aic.gov.au/publications/tandi/ti118.pdf

[4] Leopoldo Sebastián M Gomez, "El tratamiento de la Evidencia Digital", Simposio de Informática y Derecho, JAIIO 2004.

[5] United States Department of Justice, Criminal Division, Computer Crime and Intellectual Property Section – "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations", 2002. Disponible en http://www.usdoj.gov/criminal/cybercrime/searching.html

[6] Orin S. Kerr ,"Computer Records and the Federal Rules of Evidence", U.S. Department of Justice *Executive Office for United States Attorneys' USA Bulletin March 2001 Vol. 49, No.2*, 2001, Disponible en: http://www.usdoj.gov/criminal/cybercrime/usamarch2001_4.htm